

Appendix C

State of Kansas
Department of Children and Families
Information Technology Services
Technical Environment

PC, Server, Network and Business Application Requirements for Contractor's

August 23, 2012

This document is intended to aide potential contractors in their bidding process by making them aware of the Department for Children and Families (DCF) hardware and software standards. Services provided by contractors must meet the standards listed within this document that apply to the services that they provide. These standards shall include, but are not limited to, desktops (PC), servers, telecommunications, and networking. Although standards and technologies will be outlined in this document, DCF reserves the right to change these standards or technologies at any time.

The vendor is responsible for all costs associated with connecting to the DCF/State systems and must remain compatible as the technologies or systems are updated. This includes, but is not limited to, contractor site setup and installation of contractor owned equipment or software. Costs may vary depending on location, type of equipment, personnel, and other factors particular to the contractor. The bidder (contractor) is solely responsible to make themselves fully aware of the costs associated of accessing and using the system(s).

The contractor must be familiar with network wiring (Cat 5e,6,6a), firewalls (VPN tunneling/encryption), TCP/IP, Ethernet, LAN, and WAN specifications or must obtain these services from a subcontractor or partner. The State/DCF may provide and maintain (at cost to the contractor) all equipment and interoffice communication circuits to the edge of the contractor's network. All equipment from the contractor's router internal interface (contractor private side) is the contractor's responsibility. Dial-up modems or public Internet ISP connections may not be connected to a PC located on the State network.

1. PC, Server, and Network Hardware/Software (Contractor Responsibility):

A. PC Hardware/Software:

- 1) Desktop hardware must be within the current year's specifications for desktops and laptops. Currently DCF utilizes Dell PCs. Standard models include:

- OptiPlex 380, 780
- Latitude 5400, E6510

B. Server Hardware/Software:

- 1) Server hardware must meet the industry best practices for the applications to be run efficiently on them. DCF currently utilizes Dell.

C. Operating System/Application Software:

- 1) All software should conform to the DCF agency standard and be verified before connecting to the DCF network. DCF is currently utilizing Microsoft solutions for servers and desktops.
 - PC and server software standards are provided by the Information Technology Services (ITS) division within DCF and will be provided to the contractor. Desktop current standards: Windows 7, Office 2010
 - Server current standards: Windows 2008 R2 Server, SQL 2008R2, Exchange 2010 SP 1

D. Network Hardware/Software:

- 1) Network equipment should conform to DCF agency standards in regards to establishing secure network connections to and from DCF from contractor. Contractor will work with DCF to determine what is needed.
- 2) The contractor is responsible for all costs associated with networking equipment and software.

2. Security Patch and Application Release Management:

A. All hardware and software:

- 1) The vendor must maintain hardware compatibility and software release synchronization with DCF. All applications and operating systems must be current following the standards within DCF.
- 2) Service packs and security patches must be up to date. Coordination with DCF ITS division is required before patches and service packs are applied.
- 3) The contractor is responsible for all costs associated with maintaining compatible equipment and software.

3. Network Connectivity:

A. To and from the contractor:

- 1) Network connectivity to and from DCF must be done in a secure manner. Contractor will work with DCF to determine the best manner in which to provide network services between the contractor and DCF.
- 2) The contractor is responsible for all costs associated with them connecting to DCF.

- 3) DCF is connected to the State network (KANWIN) which is managed by the Office of Information Technology Services (OITS). Connections to and from the KANWIN must also be approved or coordinated with OITS.

4. Email/Data Communications:

A. To and from the contractor:

- 1) Communications between the contractor and DCF must be done so in a secure manner. These details must be approved and coordinated with DCF before any communication begins.
- 2) Communications from contractor to any non-DCF network site must be done so in a secure manner if client information is to be exchanged. These details must be approved and coordinated with DCF before any communication begins.

5. General Security:

A. Mainframe:

- 1) Top Secret access is required and arranged through the ITS security access unit at 785-296-4357 and will require a security agreement for any staff needing access.
- 2) Emulation will be TN3270.

B. Data Protection:

- 1) DCF ITS will work with the contractor to ensure data and communications between them are secure. DCF reserves the right to inspect and make recommendations in regards to the security of the contractor network connection to DCF, and will give all final approvals for the solutions.
- 2) Contractor may have a connection to the Internet for their own purposes, but network communication between the contractor's Internet traffic and DCF related traffic must be segregated by a firewall or other secure solution.
- 3) All security patches and Antivirus updates must be current and up to date on any equipment that comes in contact with data.

6. Application Software, Tools and Database

All software should conform to the DCF agency standard for business application software and custom off the shelf applications. The following are our current standards for Application software and Database.

A. Mainframe:

- 1) z/OS 1.13, z/9 BC (Business Class), processor model # 2096-R04, 718 mips, 64 MSU's - DCF, Serial number (273AA)
- 2) CICS 4.1

- 3) ROSCOE 6.0
- 4) TSO 5.9
- 5) ADABAS 8.2.4
- 6) DB2 9.02 full function mode
- 7) BCV5 2.3
- 8) CA:Gen / CE:Access
- 9) CA-Spool
- 10) COBOL enterprise version for z/OS vs 3.4.1
- 11) Natural 8.2
- 12) Attunity Connect 5.1
- 13) SAS 9.1.3

B. Windows Server

- 1) IBM WebSphere Application Server 7.0
- 2) Host Access Transformation Services HATS 7.0
- 3) IBM Rational Application Developer 7.5 / 7.6
 - RAD
 - RDz
 - RDz with EGL
- 4) IIS
- 5) IBM DB2/LUW
- 6) MS SQL Server Database 2008
- 7) IBM ClearQuest / RequisitePro 7.1.1
- 8) MS Team Foundation / Open source SubVersion edge 1.2.2
- 9) IBM System Architect
- 10) IBM Optim
- 11) CompuWare Client Vantage
- 12) CompuWare Server Vantage
- 13) CompuWare dynaTrace
- 14) EMC Imaging software Captiva / Documentum – several products, please contact ITS for further detail 6.5
- 15) Siebel Customer Order Management Administration Server 8.2
- 16) Oracle Policy automation 8.2
- 17) Oracle Business Intelligence publisher 10.2
- 18) Siebel CRM Base / Public Sector eService 8.2
- 19) Siebel Public Sector Partner Portal 8.2
- 20) Brava

7. Public Facing Website

The existing Public Internet Site is hosted by Kansas Inc., and content is posted through a FTP process. The Public Internet Site is built upon the Microsoft Office SharePoint Services 2010 platform and will be housed internally by DCF.

8. Accessibility Policy and Law - Computer Hardware, Software, Other Technologies. All products and services provided or developed as part of fulfilling this contract shall conform to:

[Section 508 of the Americans with Disabilities Act](#) requires Federal electronic and information technology to be accessible to all people with disabilities, including employees and members of the public.

[State of Kansas Web Accessibility Requirements](#) which include and exceed Section 508 standards, apply to all state agencies in Kansas.

Web accessibility regulations are based on the [Web Content Accessibility Guidelines 2.0 \(WCAG 2\)](#) – a set of standards created by the [World Wide Web Consortium \(W3C\)](#). The World Wide Web Consortium (W3C) is an international community that develops [standards](#) to ensure the long-term growth of the Web. Read about the [W3C mission](#).

The Web Content Accessibility Guidelines (WCAG 2) are organized around [four principles](#).

Online content must be:

1. Perceivable – users can access all information presented
2. Operable - users can find their way around
3. Understandable - users can understand the information
4. Robust - users can continue to access content as technologies advance

If any of these fail, some users will not be able to access your content.

9. System Interactions with current Data: Current methods used in DCF to interface with legacy applications are thru a batch FTP process or by the use of a web service. Vendor must include a recommended solution. Listed below are the current processes in use at DCF for a Web Service.

If a web service is required it must allow for the interfacing of information with DCF and outside agency legacy systems providing real-time or nearly real-time pushes of data. Current interfaces are developed as a web service that interacts through the IBM Host Access Transformation Services (HATS) tool. A minimum, a one-way data push from the solution to the appropriate legacy system, with a system confirmation returned. The HATS software allows DCF to web enable their existing CICS screens. DCF will create a web service for the different systems, provide the vendor with a mapping document and WSDL for each of the screens, provide the valid responses that the vendor may receive when calling one of these web services and what to do if an error is received. In addition, if this is the appropriate solution the vendor supplied solution must integrate with single sign-on and active directory.

10. Vendor Hosted Solutions: Any vendor hosted solutions must meet or exceed the

security and data standards that are outlined in this document. Vendors proposing a hosted solution must be able to provide at a minimum the following:

- A 3rd party audit of the proposed site completed within the past 12 months.
- All policies and procedures regarding physical security, access control, and monitoring of the site.
- Descriptions of physical security controls in place at the site (ie. perimeter fencing, CCTV, guard service, etc..)
- Complete list of all other customers hosted in the site, or other vendors who use that site.
- Documentation for HVAC environment including information on maintenance vendors and service contract details.
- Documentation on the power distribution plan within the data center including details about generator backup.
- Policies and procedures for data backup processes and security of backup media.
- COOP (Continuity of Operations Plan) for the facility.

DCF holds the right to ask for additional detail on all the above areas as well as the right to ask for additional information on hosted solutions and their environments that are specific to the vendors proposed solution.